



## **Employee and Student Electronic and Internet Use Policy**

Channing Hall provides employees and students access to the school's electronic network. This network includes Internet access, computer services, videoconferencing, computer equipment, related equipment for educational purposes and other developing resources. The purpose of this network is to assist employees in their work and to prepare students for success by giving them electronic access to a wide range of information and the ability to communicate with people throughout the world. This policy provides the rules and procedures for employees' and students' acceptable use of the Channing Hall electronic network and related issues.

### **I. Overview**

- A. The Channing Hall electronic network was established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality self-discovery activities, including homework.
- B. The Channing Hall electronic network was not established as a public access service, as a family resource, or as a public forum. Channing Hall has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- C. Parent/guardian permission is required for all Channing Hall students to use and access the Channing Hall electronic network, related services and resources. Access is a privilege — not a right.
- D. Employees and students may have access to Channing Hall electronic resources, systems and devices only after they have signed annually-required, school-approved acceptable use agreements. The school reserves the right to monitor all activity on this electronic network, including the use of the network or school devices while off school property. Students will indemnify the school for any damage that is caused by students' inappropriate use of the network.
- E. Employees and students are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities as well as the law in the use of the Channing Hall electronic network.
- F. Employees and students are personally responsible for assigned or loaned electronic devices, including loss or damage to devices and use of devices consistent with state and federal law and this policy.
- G. There may be exceptions to this policy for special circumstances, health-related reasons and emergencies, but they must be made in advance of any unapproved use by a school administrator.

## **II. Definitions**

- A. "Electronic network or services or equipment" means Internet service provided through Channing Hall, whether on or off school property and before, during and after school time and all electronic devices provided permanently or temporarily by Channing Hall to students and/or employees.
- B. "Employee" also means school volunteers, for the purpose of this policy.
- C. "Harassment" means a course of conduct which annoys, threatens, intimidates, alarms, or puts a person in fear of their safety. Harassment is unwanted, unwelcome and uninvited behavior that demeans, threatens or offends the victim and results in a hostile environment for the victim.

## **III. Generally Unacceptable Network and Media Use for Students and Employees**

- A. While utilizing any portion of the Channing Hall electronic network, unacceptable behaviors include, but are not limited to, the following employee or student activities:
  - 1. Intentionally accessing, transmitting, possessing or receiving material in violation of state law, federal law or school policy on school property or at a school-sponsored event or activity. This includes pornographic, indecent or sexually suggestive materials, weapons, controlled substances or alcohol or incendiary devices.
  - 2. Playing games, using IM, emailing, listening to music or any other activities, applications or functions during class time, unless expressly approved by a supervisor/ teacher for the educational goals of that particular course and during that particular class.
  - 3. Posting materials or information that, if acted upon, could cause damage or danger of disruption in a classroom or at a school sponsored activity.
  - 4. Engaging in personal attacks, including prejudicial or discriminatory attacks against other students, adults, or school personnel.
  - 5. Harassing another person.
  - 6. Knowingly or recklessly posting false or defamatory information about a person or organization.
  - 7. Using criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
  - 8. Using speech that is inappropriate in an educational setting or violates school rules.
  - 9. Abusing network resources such as sending chain letters or "spamming."
  - 10. Using the Channing Hall electronic network for commercial purposes, including advertising, selling, offering or providing services.
  - 11. Using the Channing Hall network for political lobbying.
  - 12. Using any wired or wireless network (including third-party internet service providers) with equipment brought from home. Example: The use of a home

computer that has not been accepted and first configured with Channing Hall software is prohibited on the network. There can be no accessing the Internet from any device not owned or set up by the school.

13. Using school equipment, network, or credentials to threaten others, or cause a disruption to the educational program.
14. Using the equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
15. Tampering, altering or deleting any software or filters that Channing Hall installs on school-owned or assigned computers unless the employee or student receives express permission to do so.
16. Loaning, selling, or disposing of Channing Hall electronic devices or property, except for those employees assigned to dispose of Channing Hall property

#### **IV. E-Mail**

- A. Employees/students may be provided with e-mail accounts for specific educational projects or activities.
- B. Employees/students will not establish or access Web-based e-mail accounts on commercial services through the school network unless such accounts have been approved for use by the individual school.
- C. Employees/students will not repost messages that were sent to them privately without the permission of the individual(s) who sent the message.
- D. Employees/students will not post FERPA-protected or private information about students or others.
- E. Employee/student email communications using the school system are not private.

#### **V. World Wide Web**

- A. Access to information for students on the Web will generally be provided through prescreened sites and in a manner prescribed by Channing Hall administration and staff.
- B. Employees and students may use the Internet and other electronic information and resources consistent with state law, federal law, and the school's required acceptable use agreement.

#### **VI. Telnet and FTP**

- A. Telnet and FTP services may be available to employees and students. However, all aspects of this policy are applicable to material accessed or downloaded.

#### **VII. Message Board/Usenet Groups**

- A. The school will provide access to selected newsgroups that relate to subjects appropriate for educational use. Messages posted locally that are in violation of this policy will be removed. The school reserves the right to immediately terminate an employee or student account if the employee/student misuses the message boards or Usenet groups.

### **VIII. Web Sites**

- A. Employee/student images taken in common areas of the school (lunchroom, school athletic events and activities, field days) may be used on the school website.
- B. Employee and student names may be used on the school website unless a parent specifically, consistent with FERPA, has denied the school permission to release student names or personal information.
- C. Material placed on student Web pages is expected to meet academic standards of proper spelling, grammar and accuracy of information.
- D. Employees/students may not use materials (graphics, text, sound, etc.) that are owned by someone else on school websites unless formal permission has been obtained from the owner of the material.
- E. All student web pages should link back to the homepage of the classroom, school, or activity as appropriate.

### **IX. Personal Safety While on the Internet**

- A. Employees/students will not share personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, or work address.

### **X. System Security**

- A. Employees and students are responsible for their individual accounts and should take all reasonable precautions to prevent use by others.
- B. Under no conditions should employees or students provide their password to another person.
- C. Employees/students must immediately notify a teacher or the system administrator if they have identified a possible security problem.
- D. Employees/students will not attempt to gain unauthorized access to any portion of the Channing Hall electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing."
- E. Employees/students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- F. Users will not attempt to access websites blocked by school policy, including the use of proxy services, software, or websites.
- G. Users will not use sniffing or remote access technology to monitor the network or other users' activity.

### **XI. Software and Files**

- A. Software is available for employees and students as an educational resource. Designated employees may upload or download software for educational purposes. No

student may install, upload or download software without permission from the school technology staff.

- B. A student's account may be limited or terminated if a student intentionally misuses software on any school-owned equipment.
- C. Files stored on the network and on individual computers are treated in the same manner as other school storage areas, such as desks and lockers. Routine maintenance and monitoring of the Channing Hall electronic network may lead to discovery that an employee or student has violated this policy or the law.
- D. Employees and students should not expect that files stored on school devices or servers are private.

**XII. Technology Hardware**

- A. Hardware and peripherals are provided as tools for employee/student use for educational purposes. Only designated employees are permitted to relocate hardware (except for portable devices), install peripherals or modify settings to equipment without the consent of the school technology staff.

**XIII. Vandalism**

- A. Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges and confiscation of school devices.
- B. Employees and students may be disciplined for vandalism of the school's electronic systems or equipment.

**XIV. Videoconference**

- A. Videoconferencing is a way that students can communicate with other students, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, students can see, hear, and speak with other students, speakers, museum personnel, etc. in real-time.
- B. Videoconference sessions may be videotaped by school personnel or by a participating school involved in the exchange in order to share the experience within our or designated buildings or schools.
- C. Students' voices, physical presence, and participation in the videoconference may be transmitted to participating sites during each session.
- D. Rules and procedures relative to acceptable use and behavior by students apply during all video conference sessions.

**XV. Due Process and Discipline for Employees and Students**

- A. The school will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the school network.
- B. In the event there is an allegation that a student has violated this policy, the student will be provided with a written notice of the alleged violation. An opportunity will be provided to present an explanation before a neutral administrator (or student will be

provided with notice and an opportunity to be heard in the manner set forth in the student disciplinary policy).

- C. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action. Following investigation and due process, student disciplinary action for policy violation(s) may include:
  - 1. Suspension or revocation of network and device privileges
  - 2. Use of school network only under direct supervision
  - 3. Suspension of network privileges
  - 4. Revocation of network privileges
  - 5. Suspension of computer privileges
  - 6. Suspension from school
  - 7. Expulsion from school and/or
  - 8. Legal action and prosecution by law enforcement
- D. If there is an allegation that an employee violated this policy, the incident will be investigated and the employee may be disciplined consistent with the Employee Handbook.

#### **XVI. Limitation of Liability**

- A. The school makes no guarantee that the functions or the services provided by or through the school network will be error-free or without defect. The school will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service.
- B. The school is not responsible for the accuracy or quality of the information obtained through or stored on the network. The school will not be responsible for financial obligations arising through the unauthorized use of the network.

#### **XVII. Additional Employee Provisions**

- A. Employees may only offer or purchase commercial products or services for educational purposes or with a supervisor's approval.
- B. Employees may only access the student instructional system or business systems for instructional purposes and/or purposes consistent with FERPA and Utah law.
- C. Consistent with state law, if a computer technician or technician finds or identifies child pornography or what the technician reasonably believes is child pornography, while in the course and scope of the individual's duties to install, maintain, troubleshoot, upgrade, or repair computer hardware, software, personal computer networks, or peripheral equipment, the technician shall do the following:
  - 1. Secure the device,
  - 2. Disconnect it from the Channing Hall network
  - 3. Exclude the individual to whom the device was assigned, as well as all other individuals with the exception of law enforcement, from the device
  - 4. Contact the head of school

5. Head of school shall contact law enforcement or a designated cyber tip line.

**XVIII. Additional Student Provisions**

- A. Students may use the system to communicate with elected representatives and to express their opinions on political or policy issues.
- B. Students will not attempt to access non-instructional school systems, such as student information systems or business systems
- C. Students will not disclose personal contact information, except to education institutions for educational purposes, companies or other entities for career development purposes, or without specific building administrative approval.
- D. Students will not agree to meet with someone they have met online.
- E. Students will promptly disclose to a teacher or other designated school employee any message received that is inappropriate or makes the student feel uncomfortable.
- F. Channing Hall's electronic network is considered a limited open forum, and therefore the school may restrict a student's speech for valid educational reasons. The school will not restrict a student's speech on the basis of a disagreement with the opinions that are being expressed.
- G. Students may not use electronic devices during standardized assessments, unless directed by state law and school supervisors.